WHAT IS CLAIMED IS:

1. A modular exponentiation calculation apparatus which utilizes a residue number system representation by a first base and a second base including sets of a plurality of integers with respect to object data C and parameters p, q, d (all integers included in both the bases are mutually primary, a product "A" of all the integers of the first base is $A > p$, $A > q$, a product "B" of all the integers of the second base is $B > p$, $B > q$, and $A \times B > C$) to obtain a calculation result $m = C^d \bmod (p \times q)$, said apparatus comprising:

a first processing unit configured to obtain a residue number system representation of a value $Cp^{dp} \times B \bmod p$ or a value with p added thereto based on a residue number system representation of a remainder value $Cp = C \bmod p$ by p of said data C and a remainder value $dp = d \bmod (p - 1)$ by $(p - 1)$ of said parameter d;

a second processing unit configured to obtain a residue number system representation of a value $Cq^{dq} \times B \bmod q$ or a value with q added thereto based on a residue number system representation of a remainder value $Cq = C \bmod q$ by q of said data C and a remainder value $dq = d \bmod (p - 1)$ by $(q - 1)$ of said parameter d;

a third processing unit configured to obtain a residue number system representation of an integer m'

congruent with C^d mod $(p \times q)$ based on both the residue number system representations obtained by said first and second processing units; and

a fourth processing unit configured to obtain said calculation result m based on a value of said integer m' obtained by converting said residue number system representation obtained by said third processing unit into a binary representation.

2. The modular exponentiation calculation apparatus according to claim 1, wherein said first processing unit performs a residue number system Montgomery multiplication of the residue number system representation of said remainder value Cp and the residue number system representation of B^2 mod p, performs a residue number system Montgomery exponentiation using said remainder value dp as an exponent portion with respect to the obtained residue number system representation, and thereby obtains the residue number system representation of the value $Cp^{dp} \times B$ mod p or the value with p added thereto, and

said second processing unit performs a residue number system Montgomery multiplication of the residue number system representation of said remainder value Cq and the residue number system representation of B^2 mod q, performs a residue number system Montgomery exponentiation using said remainder value dq as the exponent portion with respect to the obtained residue

number system representation, and thereby obtains the residue number system representation of the value $Cq^{dq} \times B \bmod q$ or the value with q added thereto

3. The modular exponentiation calculation apparatus according to claim 2, further comprising a unit configured to obtain said remainder value dp and said remainder value dq based on said parameters p, q, and d.

4. The modular exponentiation calculation apparatus according to claim 1, wherein said third processing unit performs a residue number system Montgomery multiplication of said residue number system representation obtained by said first processing unit and the residue number system representation of an inverse element $qinv = q^{-1} \bmod p$ in a modulus p of said parameter q, performs a residue number system multiplication of the obtained residue number system representation and the residue number system representation of said parameter q, performs a residue number system Montgomery multiplication of said residue number system representation obtained by said second processing unit and the residue number system representation of an inverse element $pinv = p^{-1} \bmod q$ in a modulus q of said parameter p, performs a residue number system multiplication of the obtained residue number system representation and the residue number system representation of said parameter p, performs a

residue number system addition of both obtained results of a residue number system multiplication, and obtains the residue number system representation of the integer m' as the combination with C^d in said modulus p × q.

5. The modular exponentiation calculation apparatus according to claim 4, further comprising a unit configured to convert the binary representations of said parameter p, said parameter q, said inverse element pinv, and said inverse element qinv to the residue number system representations.

6. The modular exponentiation calculation apparatus according to claim 5, further comprising a unit configured to obtain the inverse element pinv and the inverse element qinv in the modulus p of said parameter q based on said parameters p and q.

7. The modular exponentiation calculation apparatus according to claim 1, further comprising a unit configured to obtain said remainder value Cp and said remainder value Cq based on said data C and said parameters p and q.

8. The modular exponentiation calculation apparatus according to claim 1, further comprising a storage unit configured to store data of a residue number system representation depending only on said parameters p, q, d.

9. The modular exponentiation calculation apparatus according to claim 1, further comprising a

storage unit configured to store identification information i for identifying said parameters, and data of a residue number system representation depending only on parameters pi, qi, di corresponding to the identification information i.

10. The modular exponentiation calculation apparatus according to claim 1, wherein said first processing unit and said second processing unit execute at least a part of a processing at the same time.

11. The modular exponentiation calculation apparatus according to claim 1, wherein said first processing unit and said second processing unit simultaneously execute all or some of operations corresponding to elements with respect to operations to be performed for respective elements of said base.

12. The modular exponentiation calculation apparatus according to claim 1, wherein said fourth processing unit includes:

a subunit configured to convert the residue number system representation of said integer m′ obtained by said third processing unit to a binary representation; and

a unit configured to set a value of said integer m′ less than $p \times q$ obtained by the subunit or a value less than $p \times q$ obtained by subtracting a predetermined number $p \times q$ from said integer m′ not less than $p \times q$ to $m = C^d \bmod p \times q$.

13. The modular exponentiation calculation apparatus according to claim 1, wherein the number of elements of said first base is the same as the number of elements of said second base.

14. A modular exponentiation calculation method which utilizes a residue number system representation by a first base and a second base including sets of a plurality of integers with respect to object data C and parameters p, q, d (all integers included in both the bases are mutually primary, a product "A" of all the integers of the first base is $A > p$, $A > q$, a product "B" of all the integers of the second base is $B > p$, $B > q$, and $A \times B > C$) to obtain a calculation result $m = C^d \bmod (p \times q)$, said method comprising:

obtaining a first residue number system representation of a value $Cp^{dp} \times B \bmod p$ or a value with p added thereto based on a residue number system representation of a remainder value $Cp = C \bmod p$ by p of said data C and a remainder value $dp = d \bmod (p - 1)$ by $(p - 1)$ of said parameter d;

obtaining a second residue number system representation of a value $Cq^{dq} \times B \bmod q$ or a value with q added thereto based on a residue number system representation of a remainder value $Cq = C \bmod q$ by q of said data C and a remainder value $dq = d \bmod (p - 1)$ by $(q - 1)$ of said parameter d;

obtaining a third residue number system

representation of an integer m' congruent with C^d mod (p × q) based on the first and second residue number system representations; and

obtaining said calculation result m based on a value of said integer m' obtained by converting said third residue number system representation into a binary representation.

15. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein, the computer readable program code means utilizing a residue number system representation by a first base and a second base including sets of a plurality of integers with respect to object data C and parameters p, q, d (all integers included in both the bases are mutually primary, a product "A" of all the integers of the first base is A > p, A > q, a product "B" of all the integers of the second base is B > p, B > q, and A × B > C) to obtain a calculation result m = C^d mod (p × q), the computer readable program code means comprising:

computer readable program code means for causing a computer to obtain a first residue number system representation of a value Cp^{dp} × B mod p or a value with p added thereto based on a residue number system representation of a remainder value Cp = C mod p by p of said data C and a remainder value dp = d mod (p - 1) by (p - 1) of said parameter d;

computer readable program code means for causing a computer to obtain a second residue number system representation of a value $Cq^{dq} \times B \bmod q$ or a value with q added thereto based on a residue number system representation of a remainder value $Cq = C \bmod q$ by q of said data C and a remainder value $dq = d \bmod (p - 1)$ by $(q - 1)$ of said parameter d;

computer readable program code means for causing a computer to obtain a third residue number system representation of an integer m' congruent with $C^d \bmod (p \times q)$ based on the first and second residue number system representations; and

computer readable program code means for causing a computer to obtain said calculation result m based on a value of said integer m' obtained by converting said third residue number system representation into a binary representation.

16. A decryption apparatus which utilizes a residue number system representation by a first base and a second base including sets of a plurality of integers with respect to ciphertext data C and secret keys d and $N = p \times q$ (all integers included in both the bases are mutually primary, a product "A" of all the integers of the first base is $A > p$, $A > q$, a product "B" of all the integers of the second base is $B > p$, $B > q$, and $A \times B > C$) to obtain a plaintext $m = C^d \bmod (p \times q)$, said apparatus comprising:

a first processing unit configured to obtain a residue number system representation of a value $Cp^{dp} \times B \bmod p$ or a value with p added thereto based on a residue number system representation of a remainder value $Cp = C \bmod p$ by p of said data C and a remainder value $dp = d \bmod (p - 1)$ by $(p - 1)$ of said key d;

a second processing unit configured to obtain a residue number system representation of a value $Cq^{dq} \times B \bmod q$ or a value with q added thereto based on a residue number system representation of a remainder value $Cq = C \bmod q$ by q of said data C and a remainder value $dq = d \bmod (p - 1)$ by $(q - 1)$ of said key d;

a third processing unit configured to obtain a residue number system representation of an integer m' congruent with $C^d \bmod (p \times q)$ based on both the residue number system representations obtained by said first and second processing units; and

a fourth processing unit configured to obtain said plaintext m based on a value of said integer m' obtained by converting said residue number system representation obtained by said third processing unit into a binary representation.